Third International Workshop on Trustworthy Embedded Devices (TrustED 2013)

Frederik Armknecht
Universität Mannheim, Germany
armknecht@uni-mannheim.de

Jean-Pierre Seifert
Technische Universität Berlin (TUB) &
Deutsche Telekom Laboratories, DE
Jean-Pierre.Seifert@telekom.de

ABSTRACT

Cyber physical systems (CPS) feature a tight combination of and coordination between the system's computational and physical elements. A current NIST report [1] estimates that "by the end of the decade, embedded networking and computing components are projected to account for more than half of the value share in diverse sectors, including automotive, consumer electronics, avionics and aerospace, manufacturing, telecommunications, intelligent buildings, and health and medical equipment" and further conjectures that "future applications of CPS are more transformative than the IT revolution of the past three decades." While the increasing proliferation of embedded systems in general and CPS in particular provide a variety of new possibilities, new risks and challenges emerge. Due to the strong interdisciplinary character, advancement in CPS requires a new systems science that encompasses both physical and computational aspects.

The scope of the Workshop on Trustworthy Embedded Devices (TrustED) is security of embedded devices in general with focus on cyber physical systems and their environments. TrustED 2013 is a continuation of previous workshops in this series, which were held in conjunction with ESORICS 2011 and IEEE Security & Privacy 2012 (see http://trusted.trust.cased.de for details). The goal of this workshop is to bring together experts from academia and research institutes, industry, and government in the field of security and privacy in cyber physical systems.

Categories and Subject Descriptors

B.0 [**Hardware**]: General; C.2.0 [**Computer - Communication Networks**]: General—*security and protection (e.g., firewalls)*; D.4.6 [**Software**]: Operation Systems—*Security and Protection*; E.3 [**Data**]: Data Encryption; K.6.5 [**Computing Milieux**]: Management of Computing and Information Systems—*Security and Protection*

CCS'13, November 4–8, 2013, Berlin, Germany.
ACM 978-1-4503-2477-9/13/11.
http://dx.doi.org/10.1145/2508859.2509029.

Keywords

TrustED, Security, Embedded Devices, Cryptography

1. BACKGROUND AND MOTIVATION

The paradigm of ubiquitous computing and permanent, mobile connectivity has already become reality through modern technologies that allow for electronic systems to be embedded practically everywhere. Probably, the most popular example today being smart phones, additional examples include sensor nodes, smart meters, femtocells, automotive platforms, home gateways, and IPTV boxes. However, with new opportunities come new risks, affecting security and privacy. This is particularly true when embedded systems are involved, which we closely and sometimes unknowingly interact with in our daily life. Embedded devices differ significantly from "classical" systems, such as desktop PCs in various aspects:

- They have typically a variety of constraints (e.g., concerning power, memory, or processing capabilities), ruling out many classical security solutions for practical reasons.
- They can be accessed by malicious third parties with ease (e.g., physically tampered with or replaced by other devices).
- They can form a network with other embedded devices, amongst others with more powerful devices such as smart phones that function as gateways. This makes them preferable targets for network attacks (e.g., resulting in the denial of service or exhausting power).

Consequently, embedded devices and their usage in varying deployment scenarios, requires novel security methods and mechanisms. The major challenge is to develop security solutions that ensure a sufficient level of trust, security, and privacy while meeting practical requirements. Furthermore, it is well known that in order to create a secure system, system designers and developers need to consider security aspects on multiple abstraction layers, such as hardware, operating system, and application level. Particularly, for designing secure embedded systems, a careful coordination and integration of applications, operating system, and the deployed hardware is mandatory, given the fact that the options and opportunities of software and hardware are much more diverse than it is the case for the PC world.

2. SCOPE AND OBJECTIVES

Summing up, security for embedded devices is a highly interdisciplinary topic. However, this not only poses new challenges, but likewise new possibilities. A promising approach is to exploit special features in embedded devices and their environment for establishing novel secure mechanisms. Examples include the identification and deployment of new out-of-band channels, such as NFC-based schemes, the explicit use of physical properties, such as distance bounding protocols or signal fingerprinting, or secure execution environments provided by the new generation of processors. In general, the use of hardware-entangled cryptography (e.g., schemes based on physically unclonable functions - PUFs), and hardware-assisted cryptographic protocols represents a promising technological development towards trustworthy embedded devices and networks.

In this workshop, we consider selected aspects of cyber physical systems and their environments. We aim to bring together experts from academia and research institutes, industry and government to discuss and investigate the problems, challenges, and recent scientific and technological developments in this field. In this context we are particularly interested in the participation of industry representatives. The workshop includes (but is not limited to) the following topics:

- Embedded system security
- Privacy aspects of embedded systems (e.g., medical devices, electronic IDs)
- Physical and logical convergence (e.g., secure and privacy preserving facility management),
- Hardware entangled cryptography
- Foundation, development, and applications of physical security primitives (e.g., physically unclonable functions - PUFs),
- Remote attestation
- IP protection for embedded systems
- Reverse engineering
- Secure execution environments (e.g., TrustZone, TPMs, etc.) on mobile devices
- New protection paradigms for trustworthy embedded systems

3. PROGRAM COMMITTE

We are thankful to the members of our program committee:

- Liang Cai (Qualcomm, US)
- Mauro Conti (University of Padua, IT)
- Bruno Crispo (University of Trento, IT)
- Loïc Duflot (SGDN/DCSSI - Paris, FR)
- William Enck (NC State University, US)
- Wieland Fischer (Infineon, DE)
- Felix Freiling (University of Erlangen, DE)
- Jorge Guajardo Merchan (Robert Bosch LLC, US)
- Tim Güneysu (Ruhr-University Bochum, DE)
- Helena Handschuh (Cryptography Research, US)
- Xuxian Jiang (NC State University, US)
- Farinaz Koushanfar (Rice University, US)
- Peter Langendoerfer (IHP, DE)
- Refik Molva (Eurecom, FR)
- Collin Mulliner (Northeastern University, US)
- Bart Preneel (KU Leuven, BE)
- Volker Roth (Freie Universität Berlin, DE)
- Boris Skoric (Eindhoven University of Technology, NL)
- John Solis (Sandia National Laboratories, US)
- Vincent van der Leest (Intrinsic ID, NL)
- Ingrid Verbauwhede (KU Leuven, BE)
- Xinwen Zhang (Huawei Research Center, US)

4. PC CO-CHAIRS

Frederik Armknecht is an Assistant Professor for Cryptography at the University of Mannheim, Germany. His research interests include lightweight cryptography, in particular the analysis and development of new building blocks, hardware-entangled cryptography, e.g., systematizing and formalizing security properties and goals, and the design of new, practical schemes that allow for operating on encrypted data, e.g., homomorphic encryption schemes, that are tailored for practical use cases. Together with Ahmad-Reza Sadeghi, he initiated TrustED in 2011.

Jean-Pierre Seifert is a Full Professor heading the "Security in Telecommunications" group at TU Berlin. His professorship is concurrently concerned with security in telecommunications management matters at T-Labs, the R&D arm of Deutsche Telekom (DT) at TU Berlin. His main research interest is in system security with specializations in secure virtualization of operating systems and a holistic view of telecommunication security, which includes hardware security. Under his leadership, his research group is directly transferring its research results into high-security DT products for the German government. In 2002, he was honoured by Infineon with the award "Inventor of the Year" and received two Intel Achievement Awards in 2005 for his new CPU security instructions for Intel microprocessors.

5. REFERENCES

[1] *Strategic R&D Opportunities for 21st Century Cyber-Physical Systems.* NIST-Report, 2013. Available at `http://www.nist.gov/el/upload/12-Cyber-Physical-Systems020113\_final.pdf`.